

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08018582 A

(43) Date of publication of application: 19 . 01 . 96

(51) Int. Cl

H04L 12/40

H04L 12/46

H04L 12/28

(21) Application number: 06149722

(71) Applicant: TOSHIBA CORP

(22) Date of filing: 30 . 06 . 94

(72) Inventor: ANDO ARATA

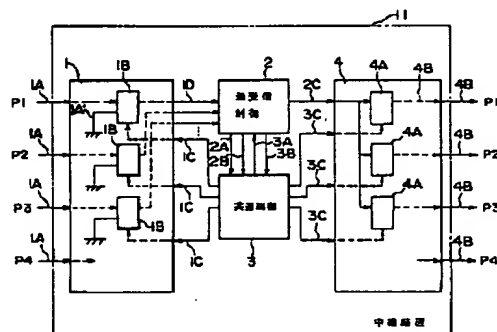
(54) NETWORK REPEATER AND NETWORK SYSTEM USING IT

(57) Abstract:

PURPOSE: To prevent the use of the network by an illegal terminal equipment by applying enable/disable control to each port as required.

CONSTITUTION: A network repeater 11 has a reception enable/disable circuit 1B respectively provided corresponding to ports P1-P4, and a transmission enable/disable circuit 4A and the transmission or reception of the circuits is subject to enable/disable control by a command from a terminal equipment. When, for example, a manager of the network or the like finds out the existence of an illegal terminal equipment by monitoring a terminal equipment address or protocol on the network, the reception of the port corresponding to the network in which the illegal terminal equipment is in existence is inhibited.

COPYRIGHT: (C)1996,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8 - 1 8 5 8 2

(43) 公開日 平成 8 年 (1996) 1 月 19 日

(51) Int. Cl. ⁶

識別記号

庁内整理番号

F I

技術表示箇所

H04L 12/40

12/46

12/28

H04L 11/00

320

310

C

審査請求 未請求 請求項の数 3 O L (全 7 頁)

(21) 出願番号 特願平 6 - 1 4 9 7 2 2

(22) 出願日 平成 6 年 (1994) 6 月 30 日

(71) 出願人 0 0 0 0 0 3 0 7 8

株式会社東芝

神奈川県川崎市幸区堀川町 7 2 番地

(72) 発明者 安東 新

東京都青梅市末広町 2 丁目 9 番地 株式会

社東芝青梅工場内

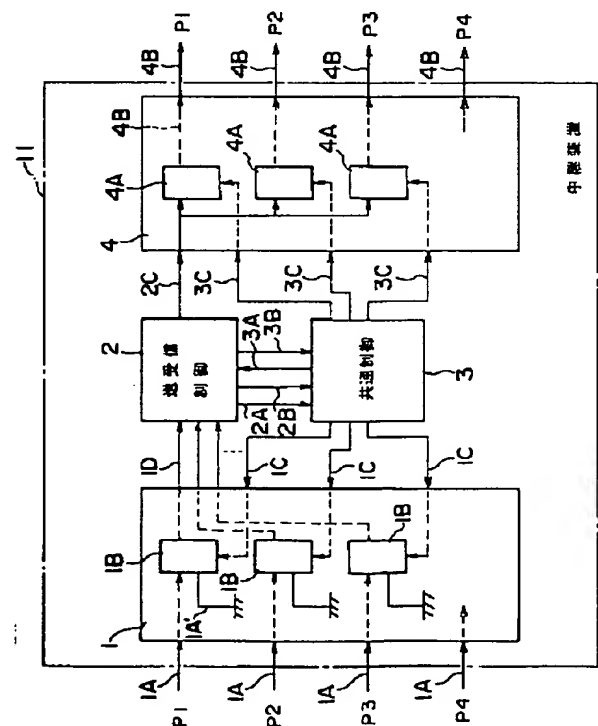
(74) 代理人 弁理士 鈴江 武彦

(54) 【発明の名称】 ネットワーク中継装置およびこれを使用したネットワークシステム

(57) 【要約】

【目的】 各ポートを必要に応じてイネーブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止を実現する。

【構成】 ネットワーク中継装置 11 は、ポート P1～P4 にそれぞれ対応して設けられた受信イネーブル／ディスエーブル回路 1B、および送信イネーブル／ディスエーブル回路 4A を有しており、これら回路は端末からのコマンドによってその送信動作または受信動作がイネーブル／ディスエーブル制御される。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができる。



【特許請求の範囲】

【請求項 1】 ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とするネットワーク中継装置。

【請求項 2】 ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とするネットワーク中継装置。

【請求項 3】 ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、

前記各ネットワーク中継装置は、ネットワークに接続される複数のポートと、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【 0 0 0 1 】

【産業上の利用分野】 この発明は、サーバ、ブリッジ、ルータ、またはゲートウェイ等のネットワーク中継装置、およびそのネットワーク中継装置を使用したネットワークシステムに関する。

【 0 0 0 2 】

【従来の技術】 一般に、複数の LAN（ローカルエリアネットワーク）や WAN（ワイドエリアネットワーク）を相互に接続する方式として、ブリッジ、ルータ、ゲートウェイ等のネットワーク中継装置が知られている。

【 0 0 0 3 】 これら各ネットワーク中継装置は、ネットワークセグメントに接続される複数のポートを有しており、それらポート間で受信パケットの転送を行うことに

よってネットワークセグメントを相互接続する。ポート間の転送は次のようなフィルタリング処理によって行われる。

【 0 0 0 4 】 例えば、第 1 および第 2 の 2 つのポートを有するブリッジ装置が第 1 ポートでパケットを受信した時には、その受信したパケットの宛先アドレスによって指定されるデータステーションが接続されているポートが調べられ、そのポートに受信パケットが転送される。もしそのポートが受信ポートであれば、受信パケットは廃棄される。

【 0 0 0 5 】 このようなネットワーク中継装置においては、ネットワークシステムの安全性を確保するために、次のようなポート制御が行われている。すなわち、ネットワークに接続されたあるデータステーションが故障し、それがデータ送信し続けことによってネットワーク全体に影響が及ぶことを防止するために、ネットワーク中継装置は、ある一定以上のデータ長を検出した場合、そのポートを論理的に切り離す機能を有している。

【 0 0 0 6 】 また、信号／衝突検出型のネットワークでは、ある単位時間中に所定回数以上の衝突を検出した場合に、該当するポートを切り離す機能を持つ中継装置もある。

【 0 0 0 7 】 しかしながら、このような従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできない。

【 0 0 0 8 】 このため、ネットワーク上に不正端末が存在することが発見された場合であっても、その不正端末が正常な手続きでアクセス動作している限りはポート制御機能は働かない。したがって、不正端末によるネットワークアクセスを防止することはできなかった。

【 0 0 0 9 】 また、従来のネットワークの形態は、バス、スター、リングの組み合わせでのみ可能であり、一部のネットワークが故障した場合の迂回路形成等が困難であった。

【 0 0 1 0 】

【発明が解決しようとする課題】 従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできなかった。このため、必要に応じてポートを動的に制御する事ができず、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができない欠点があった。

【 0 0 1 1 】 この発明はこの様な点に鑑みてなされたもので、各ポートを必要に応じてイネーブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができるネットワーク中継装置を提供することを目的

とする。

【 0 0 1 2 】

【課題を解決するための手段および作用】この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とする。

【 0 0 1 3 】このネットワーク中継装置においては、外部からのコマンドによって任意のポートの送信動作または受信動作をイネーブル／ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などをコマンドによって禁止することができる。

【 0 0 1 4 】また、この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とする。

【 0 0 1 5 】このネットワーク中継装置においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されており、不正端末以外の他の端末の送受信に影響を与えることなく、不正端末のネットワークアクセスだけを防止することができる。

【 0 0 1 6 】また、この発明は、ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、前記各ネットワーク中継装置は、ネットワークに接続される複数のポートと、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とする。

【 0 0 1 7 】このネットワークシステムにおいては、複

数のネットワーク中継装置を例えばメッシュ状に結合することにより複数のデータ転送経路が設けられており、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル／ディスエーブル制御を行っておき、障害発生やトラフィック状態に応じてその経路を動的に変更するといった運用が可能になる。

【 0 0 1 8 】

【実施例】以下、図面を参照してこの発明の実施例を説明する。図 1 にはこの発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成が示されている。ネットワーク中継装置 1 1 は 2 以上のポートを持つマルチポートタイプの中継装置であり、ここでは、ネットワーク中継装置 1 1 が図示のように 4 つのポート P 1 ~ P 4 を持ち、それらポート P 1 ~ P 4 がそれぞれ LAN セグメント 1 2 ~ 1 5 に接続されている場合を例示して説明する。

【 0 0 1 9 】LAN セグメント 1 2 ~ 1 5 の各々には、データ処理端末が接続されている。これらデータ処理端末は、ワークステーションやパーソナルコンピュータ、またはミニコンピュータ等によって実現されるものであり、対応する LAN セグメントを介して相互に通信を行うと共に、ネットワーク中継装置 1 1 を介して他の LAN セグメント上のデータ処理端末などと通信を行う。

【 0 0 2 0 】ネットワーク中継装置 1 1 は、例えば、ネットワークサーバ、リピータ、ブリッジ、ルータ、またはゲートウェイ等を構成するものであり、LAN セグメント 1 2 ~ 1 5 間の相互接続、または WAN、公衆回線網等に接続するため等に使用される。

【 0 0 2 1 】このネットワーク中継装置 1 1 は、ポート P 1 ~ P 4 を個別にイネーブル／ディスエーブル制御するためのポートイネーブル／ディスエーブル制御ユニット 1 1 1 を備えている。ポートイネーブル／ディスエーブル制御ユニット 1 1 1 は、斜線で図示されている LAN セグメント上の遠隔端末や、またはネットワーク中継装置 1 1 に直接接続された管理装置などからの要求に応じて、4 つのポート P 1 ~ P 4 それぞれの受信動作および送信動作を個別に制御する事ができる。

【 0 0 2 2 】次に、図 2 を参照して、ネットワーク中継装置 1 1 の具体的な構成の一例を説明する。ネットワーク中継装置 1 1 は、図示のように、受信部 1、送受信制御部 2、共通制御部 3、および送信部 4 を備えている。

【 0 0 2 3 】受信部 1 はポート P 1 ~ P 4 それぞれからのパケット受信データ 1 A を受信するためのものであり、ポート P 1 ~ P 4 にそれぞれ対応して設けられた 4 つの受信データイネーブル／ディスエーブル回路 1 B を有している。

【 0 0 2 4 】これら 4 つの受信データイネーブル／ディスエーブル回路 1 B は、それぞれ対応するポート P 1 ~ P 4 からパケットデータ 1 A を受信する回路であり、イネーブル／ディスエーブル信号 1 C によってその受信動

10

20

30

40

50

作が個別に許可／禁止されるように構成されている。

【 0 0 2 5 】すなわち、受信データイネーブル／ディスエーブル回路 1 B はイネーブルの時には受信データ 1 A を選択し、ディスエーブルの場合には接地電位 1 A[′] を選択する。これら 4 つの受信データイネーブル／ディスエーブル回路 1 B からの受信データ出力 1 D は、送受信制御部 2 に共通に供給される。

【 0 0 2 6 】送信部 4 は、ポート P 1 ～ P 4 それぞれからパケットデータ 4 B を送信するためのものであり、ポート P 1 ～ P 4 にそれぞれ対応して設けられた 4 つの送信データイネーブル／ディスエーブル回路 4 A を有している。これら 4 つの送信データイネーブル／ディスエーブル回路 4 A は、それぞれ対応するポート P 1 ～ P 4 からパケットデータ 4 B を送信するために設けられた回路であり、イネーブル／ディスエーブル信号 3 C によってその受信動作が個別に許可／禁止されるように構成されている。

【 0 0 2 7 】4 つの送信データイネーブル／ディスエーブル回路 4 A には、送受信制御部 2 からの送信データが共通に供給され、相手先端末に対応するポートに対応する送信データイネーブル／ディスエーブル回路 4 A から出力される。

【 0 0 2 8 】送受信制御部 2 は、受信データイネーブル／ディスエーブル回路 1 B から受信した受信データの制御、および送信データイネーブル／ディスエーブル回路 4 A に出力する送信データの制御を行うためのものであり、通常、クロックリカバリ回路、F I F O バッファ、メモリなどから構成される。また、送受信制御部 2 は、受信データイネーブル／ディスエーブル回路 1 B の制御のために、受信データ 2 A、および受信クロック 2 B を利用して、共通制御部 3 に受信したコマンドなどを送信する。

【 0 0 2 9 】共通制御部 3 は、受信データイネーブル／ディスエーブル回路 1 B、および送信データイネーブル／ディスエーブル回路 4 A をイネーブル／ディスエーブル制御するためのものであり、送受信制御部 2 から転送されるコマンドに応じて動作する。

【 0 0 3 0 】この共通制御部 3 は、通常、シリアルコントローラ、データシリアル／パラレル変換回路、C P U、メモリなどから構成される。また、3 4 A、3 B は共通制御部 3 が送受信制御部 2 との通信にしようするデータ、クロックなどである。

【 0 0 3 1 】次に、図 2 の中継装置 1 1 の動作を説明する。通常のデータ転送時においては、各ポートの受信イネーブル／ディスエーブル回路 1 B は制御信号 1 C によって受信データ 1 A を選択するイネーブル状態に設定されている。また、各ポートの送信イネーブル／ディスエーブル回路 4 A も制御信号 3 C により送信イネーブル状態に設定されている。

【 0 0 3 2 】ここで、ネットワークの管理者などが別途

ネットワークに接続された装置、または中継装置 1 1 の持つ機能などによって、ネットワーク上に不正端末の存在を発見した場合、または障害／トラフィックに応じてあるポートのイネーブル／ディスエーブル制御により経路を変更したい場合を考える。

【 0 0 3 3 】この場合、ネットワーク管理者は、ネットワーク 1 3 上の所定の端末などを利用して、中継装置 1 1 に対してコマンドを発行し、イネーブル／ディスエーブルするポート番号などを通知する。

【 0 0 3 4 】この時、ポート P 2 から受信した中継装置 1 1 宛のコマンドは送受信制御部 2 を経由して共通制御部 3 に入力される。共通制御部 3 は、受信コマンドを解析し、それが上記コマンドであった場合には、受信制御信号 1 C または送信制御信号 3 C、あるいはそれら両方の制御信号を用いて、送受信のイネーブル／ディスエーブル制御を行う。

【 0 0 3 5 】コマンドによってポート P 1 の受信動作をディスエーブルすることが指定されると、受信部 1 においては、制御信号 1 C により受信イネーブル／ディスエーブル回路 1 B の入力を受信データ 1 A から 1 A[′] に切り替えられ、その受信動作が禁止される。

【 0 0 3 6 】この構成においては、端末からコマンドなどによって任意のポートの送信動作または受信動作をイネーブル／ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができ、ネットワークの信頼性の向上を図る事ができる。

【 0 0 3 7 】次に、図 3 を参照して、受信イネーブル／ディスエーブル回路 1 B 周辺の他の回路構成を説明する。すなわち、この図 3 においては、図 2 の構成に加え、各ポート毎にシリアル／パラレル変換回路 1 E、パラメータレジスタ 1 F、および復旧回路 1 I を備えている。

【 0 0 3 8 】シリアル／パラレル変換回路 1 E は、受信イネーブル／ディスエーブル回路 1 B と並列に設けられており、受信イネーブル／ディスエーブル回路 1 B のイネーブル／ディスエーブル状態に関係なく受信データ 1 A を受信し、それをシリアルデータからパラレルデータに変換し、パラメータレジスタ 1 F の設定値と比較する。この比較動作は、受信データの送信元アドレスが、パラメータレジスタ 1 F に予め設定された受信許可端末のアドレスと一致するか否かを検出するために行われる。

【 0 0 3 9 】復旧回路 1 I は、制御信号 1 C により受信ディスエーブルが宣告されていても、シリアル／パラレル変換回路 1 E から一致検出信号 1 H が発生された時には受信イネーブル／ディスエーブル回路 1 B をイネーブ

7

ル状態に設定する回路である。

【0040】すなわち、この図3の構成においては、例えばポートP1が受信ディスエーブルの場合においては、制御信号1C（図3では1J）により受信データ1Aは無視され、1Dには受信データは出力されない。しかし、この状態に於いても、受信データ1Aは常にシリアル／パラレル変換回路1Eにて受信されており、その送信元アドレス（または、送信先アドレスなど）のモニタが行われている。予め登録された各端末の物理アドレスはレジスタ1Fに設定されており、シリアル／パラレル変換回路1Eのアドレス値と常に比較される。

【0041】両者が合致した場合には、信号1Hにてアドレスの一致が復旧回路1Iに通知され、仮に共通制御部3から受信ディスエーブル信号1C（ここでは、1C2）が発生されていても、復旧回路1Iは正当な端末からのデータであると判断し、受信イネーブル／ディスエーブル回路1Bをイネーブル状態に切り替える。

【0042】この場合、受信イネーブル／ディスエーブル回路1Bの受信データの先頭がカットされる危険があるので、ディスエーブル状態であっても受信データを保持するバッファを受信イネーブル／ディスエーブル回路1Bに設けるなどの手法を採用する事が好ましい。この場合、その受信バッファの内容はポートがイネーブルであれば読み出され、ディスエーブルであれば読み出されない。

【0043】この構成においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されているので、不正端末以外の他の端末の送受信に影響を与えることなく、不正端末のネットワークアクセスだけを防止することができる。

【0044】次に、図4を参照して、図2または図3の構成を持つネットワーク中継装置11を用いたネットワークシステムの構築例を説明する。このネットワークシステムにおいては、複数のネットワーク中継装置11が

8

LANセグメントを介してメッシュ状に結合されており、これによって、あるLANセグメント上の端末から他のLANセグメント上の端末までのデータ転送経路が複数設定されるようになっている。

【0045】この場合、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル／ディスエーブル制御を行っておき、障害発生やトラフィック状態に応じて、コマンドによるポートのイネーブル／ディスエーブル制御を行ってその経路を自動的にまたは人為的に変更するといった運用を行うことが可能になる。

【0046】

【発明の効果】以上のように、この発明によれば、各ポートを必要に応じてイネーブル／ディスエーブル制御できるようになり、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことが可能となる。

【図面の簡単な説明】

【図1】この発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成を示すブロック図。

【図2】図1に示したネットワーク中継装置の具体的構成の一例を示すブロック図。

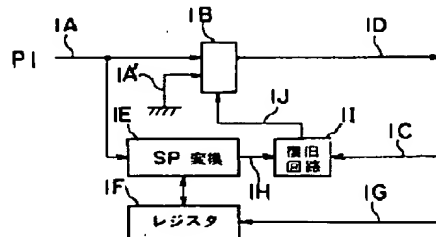
【図3】図1に示したネットワーク中継装置の他の具体的構成の一例を示すブロック図。

【図4】図1のネットワーク中継装置を多数用いて構成したネットワークシステムの一例を示す図。

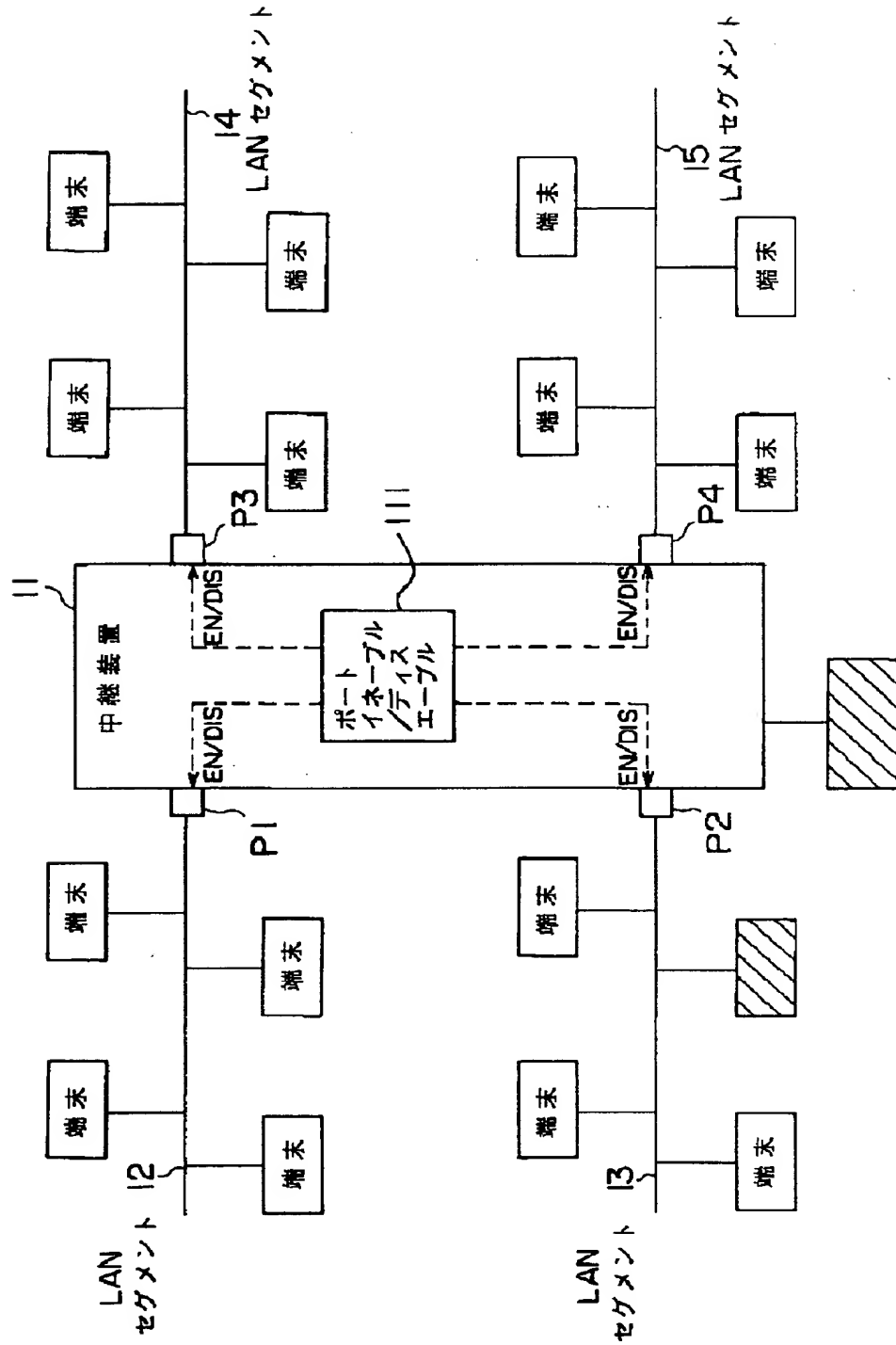
【符号の説明】

1…受信部、1B…受信イネーブル／ディスエーブル回路、1E…シリアル／パラレル変換回路、1F…パラメータレジスタ、1I…復旧回路、2…送受信制御部、3…共通制御部、4…受信部、4A…送信イネーブル／ディスエーブル回路、11…ネットワーク中継装置、12、13、14、15…LANセグメント、P1、P2、P3、P4…ポート。

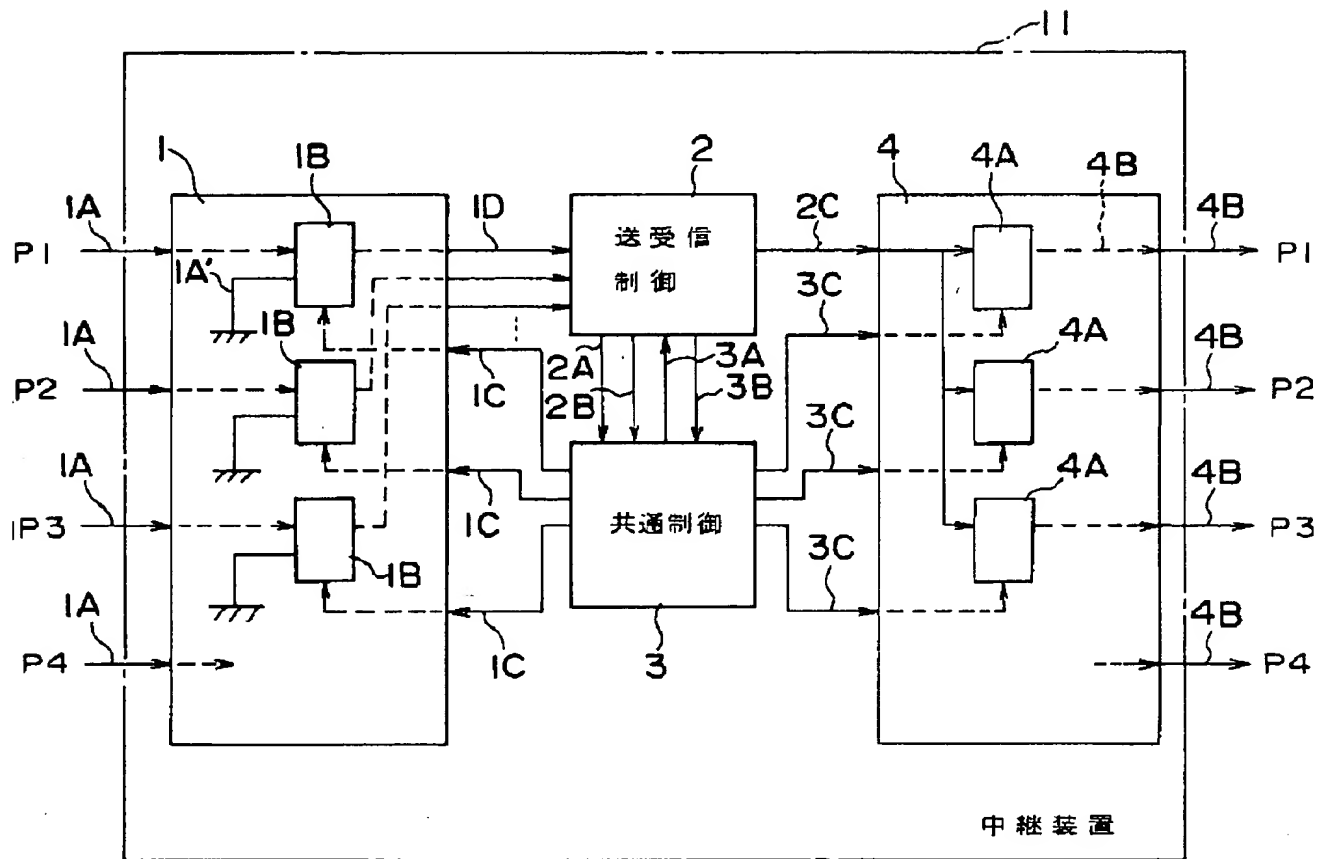
【図3】



【 図 1 】



【図 2】



【図 4】

